REMARKS

Applicants hereby reply to the Office Action dated September 22, 2005 within the shortened statutory three month period for reply. Claims 1-14 were pending in the application and the Examiner rejects claims 1-14. Applicants cancel claims 2, 3 and 9 without prejudice to filing one or more claims having similar subject matter. Reconsideration of the pending claims is requested. The amendments are adequately supported in the originally-filed specification, drawings and claims.

Rejection under 35 U.S.C. § 103(a)

The Examiner rejects claims 1-14 under 35 U.S.C. § 103(a) as being unpatentable over Applicants' own admissions in view of Gershman et al., U.S. Patent No. 6,199,099 ("Gershman"), and further in view of McGinty, WO 2001/52078 A1 ("McGinty"). Applicants respectfully traverse these rejections. Applicants also disagree that Applicants have provided such an admission.

The Examiner asserts that "the background section of the specification discloses that PDA's, portals, channels, refreshing and downloading, synchronizing of data and applications, interrogating and selection embedded links, and SSL protocols" (page 4). Applicants have outlined, in the Background section, several known methods for downloading data to a PDA device to show the deficiencies of these known methods relating to secure content. While claims 1, 4, 6 and 8 may include elements of known methods as the Examiner has suggested, the presently claimed invention includes additional unique method steps to ensure content security for a PDA device.

Because access to secure content in an online environment is maintained at the server level, there has been no need for prior art devices to maintain content security at the device level. For example, if a user would like to view his credit card balance through the issuing bank's Internet site, the site server would verify the identity of the user prior to providing access to view such content. Most PDA devices have been designed to allow a user to operate the device to view web site content while in an offline state. The user defines the specific content (channels) to download, and when the device is connected to the Internet, the selected channels are downloaded and saved within the device's memory. Thereafter, the user may view the content in an offline state as if connected to the Internet. However, because access to secure content is

normally controlled at the server level, there has not been a way to ensure that content remains secure when it is stored locally and access is no longer governed by a server.

The presently claimed invention overcomes the shortcomings of the prior art described in the Background section of the instant application by providing secure content in an encrypted form, wherein the content remains encrypted when it is stored on the PDA device. Furthermore, the isolation of imbedded links enables the PDA portal to continue to process the retrieval of linked content, while maintaining the secure content in an encrypted state. Otherwise, the PDA portal would not be able to read the links from the encrypted content without first decrypting it, leading to an increased risk of compromising the secure content.

The Examiner further states that the Applicants do not disclose isolating embedded links. However, the Examiner asserts that McGinty discloses isolating embedded links. Applicants respectfully disagree with the Examiner. McGinty discloses a system for eliminating "dead links" from documents containing hyperlinks to other documents. Because the Internet is dynamic, hyperlinks often become outdated or unusable when documents are removed, renamed, or moved to a new server location. McGinty is limited to a system that separates a first document into hyperlink elements and non-hyperlink elements. The separated hyperlinks are then tested to determine if they are valid. The valid links are added to a list and the McGinty system generates a second document including the non-hyperlink elements and the hyperlinks from the list of valid links. The second document is then provided for a client.

The Examiner next states that "it would have been obvious to one of ordinary skill in the art at the time of the invention to add the technique of identifying and isolating embedded hyperlinks as taught by McGinty with the Applicants' discussion regarding the features and uses of a standard PDA because isolating and removing or encrypting the hyperlinks increases the security of the data transmissions between the PDA and the information providing device" (page 4, paragraph 2).

Applicants assert that McGinty does not disclose or suggest the isolation of hyperlinks for the purpose of security. More specifically, the isolation of hyperlinks, as taught by the presently claimed invention, does not itself render the content more secure; however, it is a necessary step in assuring that all linked content can be collected without decrypting the content, thereby leaving the content susceptible, as previously described. Applicants assert that McGinty separates hyperlinks for the purpose of testing the validity of the hyperlink, which does not

render obvious the isolation of hyperlinks for the specific purpose as disclosed by the presently claimed invention.

The Examiner next asserts that Gershman "discloses a hardware device separate from the PDA for encryption and decryption of sensitive data transmitted to the wireless device" (page 4, paragraph 3). Gershman generally discloses an encryption device; however, Gershman fails to describe the functionality of the device. As previously stated, there are a number of encryption techniques and devices known in the art; however, Gershman only discloses an encryption device without specific disclosure as to the functionality of the device. Moreover, the Gershman encryption device is positioned between the client and the portal server in order to encrypt data that is collected by the portal server, prior to transmitting the encrypted data to the client. This configuration leaves content collected by the portal server susceptible to unauthorized access from the time the content is collected to the time it is received by the encryption device. This is contrary to the disclosure of the presently claimed invention, wherein the PDA portal does not connect directly with the content source, but instead sends a request to the encryption device. In this manner, the content is encrypted prior to being received by the PDA portal server where content may be most susceptible to unauthorized access. As such, Gershman does not disclose or suggest at least, "an encryption device, which is configured to: isolate imbedded links by facilitating a secure connection to said source using a negotiated encryption key, securing said portion of said content, receiving encrypted content which is an encrypted portion of said content, decrypting said encrypted content, interrogating said content, isolating said imbedded links, re-encrypting said portion of said content and transmitting said imbedded links and said encrypted content to said PDA portal," as similarly recited by independent claims 1, 4, 6, 8, 11, 13 and 14.

Claims 5, 7, 10 and 12 depend from independent claims 1, 4, 6, 8, 11, 13 and 14. Claims 5, 7, 10 and 12 are differentiated from the cited references for at least the same reasons as set forth above, as well as their own respective features.

Applicants respectfully submit that the pending claims are in condition for allowance. No new matter is added in this Reply. The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. **19-2814**. Applicants invite the Examiner to telephone the undersigned, if the Examiner has any questions regarding this Reply or the present application in general.

Respectfully submitted,

Dated: 11/22/05

By: _____
Howard Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com